PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 : G11B 20/10 — A1

(11) International Publication Number: WO 89/ 08915

(43) International Publication Date: 21 September 1989 (21.09.89)

(21) International Application Number: PCT/GB89/00293

(22) International Filing Date: 20 March 1989 (20.03.89)

(31) Priority Application Number: 8806452

(32) Priority Date: 18 March 1988 (18.03.88)

(33) Priority Country: GB

(71) Applicant *(for all designated States except US)*: IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY & MEDICINE[GB/GB]; Exhibition Road, South Kensington, London SW7 2AZ (GB).

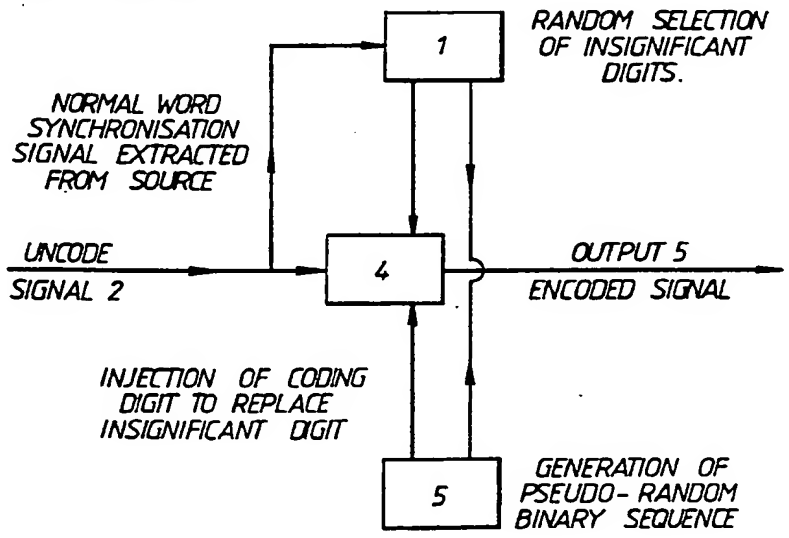
(72) Inventor; and
(75) Inventor/Applicant *(for US only)* : TURNER, Laurence, Frank [GB/GB]; The Croft, 4 Barrels Down Road, Bishops Stortford, Hertfordshire CM23 25U (GB).

(74) Agent: SHINDLER, Nigel; Batchellor, Kirk & Eyles, 2 Pear Tree Court, Farringdon Road, London EC1R 0DS (GB).

(81) Designated States: AT (European patent), AU, BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent), US.

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DIGITAL DATA SECURITY SYSTEM



(57) Abstract

A method of inserting an identification code into a digitally encoded signal such as that used in compact disc recording. A series of binary word locations in the material are selected, preferably at random, for modification by substituting a replacement digit or digits for one or more insignificant digits of the word. This allows subsequent identification of copies of the recorded material, by comparison with a copy of the random sequence or sequences used to determine the locations and values of the replacement digits. The method can also be applied to coding schemes which do not have a defined word structure, such as delta modulation, in which case digits can be replaced completely randomly without regard to relative significance.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**FR**	France	**ML**	Mali
AU	Australia	**GA**	Gabon	**MR**	Mauritania
BB	Barbados	**GB**	United Kingdom	**MW**	Malawi
BE	Belgium	**HU**	Hungary	**NL**	Netherlands
BG	Bulgaria	**IT**	Italy	**NO**	Norway
BJ	Benin	**JP**	Japan	**RO**	Romania
BR	Brazil	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SN**	Senegal
CH	Switzerland	**LI**	Liechtenstein	**SU**	Soviet Union
CM	Cameroon	**LK**	Sri Lanka	**TD**	Chad
DE	Germany, Federal Republic of	**LU**	Luxembourg	**TG**	Togo
DK	Denmark	**MC**	Monaco	**US**	United States of America
FI	Finland	**MG**	Madagascar		

"Digital Data Security System"

This invention relates to a system for security encoding of digitally recorded data.

A need exists for a security system which facilitates the identification of the source of recorded material with a high degree of certainty. This is increasingly required as facilities for high quality unauthorised copying of recorded material such as from compact discs and video tapes become more readily available on the market.

The invention also finds applications in the field of speaker identification from a digital recording of an individual's voice so that it may be recognised on subsequent encounters. Thus, it has application in remote communications for confirming the identity of a caller.

According to the present invention there is provided a method of inserting an identification code in digitally recorded material, comprising;

selecting binary word locations in the digitally recorded source material and replacing at least one insignificant digit of each selected digital word with a respective replacement digit taken from an independently generated sequence.

Preferably the binary word locations are selected at equal time intervals, or in accordance with a predetermined repeating sequence of time intervals, or in accordance with a predetermined random or pseudo-random sequence of time intervals.

The independently generated sequence may comprise a series of replacement digits which all have the same value or form a regularly repeated pattern or alternatively it may also be random or pseudo-random.

The invention also provides a method of inserting an identification code into digitally encoded material which

is applicable to delta-modulated signals consisting of a series of "one bit" words of equal significance, as well as those in which the digits are divided into groups or words within which the digits are of varying significance, the method comprising, generating a first random or pseudo-random identification sequence of binary digits, selecting binary locations in the digitally recorded source material according to a second random or pseudo-random sequence, and replacing the digit at the selected binary location with a digit from the said identifying sequence.

The present invention also provides apparatus for encoding digitally recorded material for identification purposes, said apparatus comprising:

means for selecting at least one set of binary word locations in the source material and means for replacing at least one insignificant digit of each selected digital word, with a respective predetermined replacement digit.

Preferably the apparatus also comprises means for generating further random or pseudo-random sequences, for generating the said replacement digits and/or for determining the selection of digits to be replaced in each word.

The invention further provides apparatus for decoding digital recordings which have been encoded as aforesaid comprising means for detecting digits located at the random time intervals used in the encoding process, means for holding a copy of the random or pseudo-random identifying sequence used in the encoding, means for comparing the located insignificant digits with the held random or pseudo-random identifying sequence, and means for detecting a pre-selected level of agreement therebetween.

The expression "insignificant digit" means a data bit which can be changed without noticeable detriment to the quality of reproduction of the source material.

The digits selected for replacement are preferably the least significant digits of the selected words, as such alteration may be effected without detriment to the quality of reproduction from the recorded material. However, it is also possible to replace the next significant digit, thus providing an additional layer of security in the system. The overriding criterion is, of course, that any effect on the reproduction from the recorded material should be unnoticeable. This can be achieved by ensuring that the changed digits, both least significant and digits of higher significance, are sufficiently far apart.

In practice, a random or pseudo-random sequence of pulses is used to replace certain of the least significant digits, thus providing a first layer of randomisation. The random selection of the least significant digits to be replaced provides a second layer of randomisation. The degree of complexity of the encoding may be increased by replacing randomly selected least and next least significant digits in different words by digits generated from a random or pseudo-random sequence of pulses, or by digits drawn respectively from two different pseudo-random sequences.

In general terms, then, recorded material will be converted into PCM format, for example, for digital recording and storage. In this format, word synchronisation exists, so that both the encoding and subsequent decoding means can accurately recover analogue samples from the appropriate representative digital words. In this invention, certain binary words are selected randomly and then the least (usually) significant digits of the selected words are replaced on a one-for-one basis by the digits of a long pseudo-random sequence. However, for the avoidance of doubt, it should be noted that the invention is not restricted in its application to PCM format: it may also be applied to other forms of coding such as differential PCM and delta modulation.

The pseudo-random sequence may be of a conventional type, having associated correlational properties. The identifying apparatus will, then, examine digits separated by the randomly selected time intervals and compare, for the purpose of identification, these digits with a pseudo-random sequence identical to that inserted during encoding for the purpose of identification.

The invention will now be described, by way of example, with reference to the accompanying diagrams, of which:

Figures 1 and 2 are diagrammatic representations of signals to be subjected to the encoding method of the invention; and

Figure 3 is a diagrammatic representation of the encoding step of the invention; and

Figure 4 represents the decoding step.

A typical digital signal consisting of a series of words, which may be subjected to the identification coding of the invention, is shown in Figure 1. For the purposes of illustration, the words are shown as having eight bits, and of course in a practical application such as compact disc recording, the word synchronism is already provided in the system.

As illustrated in Figure 1, the bits of most significance are at the "left-hand" end of each word, whilst the bits of lower significance, which may be subject to alteration without serious detriment to the output signal, are located towards the right-hand end of the word. Considering the illustrated signal of Figure 2 as a typical portion of a total signal to be encoded, in a preferred form of the invention, a first selection is made, of the words to be altered, which may for example be words 1, 2 and 6 of the series shown, and then a further selection is made of the particular insignificant digits to be altered within those words. In practice, the selection of words will of course

be carried out sequentially, at predetermined intervals of time which may be regular intervals, or may of course be set in accordance with the output of a random number generator. As each word to be altered is encountered in the signal, a further "choice" will be made to determine which of the insignificant digits in each case should be replaced.

In the simplest form of the invention, only one digit, for example the least significant digit, will be changed to a predetermined value (for example to a value "1") but in order to achieve a more secure coding scheme, the number of insignificant digits that is altered in each word may be different, and the values to which they are altered may also be different, in accordance with another randomly generated sequence.

Although the process is described above in terms of a "two-step" sequence of operations, it will also be appreciated that the digit selection could be carried out in effect as a "single-step" process. For example, as illustrated in Figure 3, the whole series of eight bit words could be regarded as a continuous "bit-stream", the digits being selected on a continuous basis. In Figure 2, if the leftmost bit is regarded as bit one of the complete stream, the arrows indicate the selection of digits 5, 7, 8, 15, 16, and 48 for alteration. In order to implement this, a "random number" count is made of the binary digits representing the encoded signal, starting at the "left" in the drawing, and beginning the count with the most significant digit of any binary word. Then, when the count reaches each of the numbers (5, 7, 8, 15, 16 and 48 in the illustrative example) corresponding to the positions of the digits to be replaced, the output from some random or pseudo-random sequence is taken and used to replace the selected digit in the binary representation of the encoded material.

In addition, in some types of digital encoding

schemes, such as delta modulation, there is no word structure as such, although each individual "bit" can be regarded as a "one bit word", since all digits are of equal significance, and taken individually, their significance is low. Thus if one considers the example of Figure 2 as a continuous bit stream of a delta modulated signal, exactly the same process of selection of bits to be altered can be carried out as explained above, except of course that the count leading to the location of digits to be replaced can be started at any point. Thus in Figure 3, bits 5, 7, 8, 15, 16, and 48 of the signal have been altered, but it would equally be possible to alter (for example) a sequence such as 1, 7, 10, 15, 25, 27, 36 ..., without any regard to relative "significance".

An example of coding apparatus is shown in Figure 3, in which unit 1 uses the normal word synchronisation available in the digitally recorded source signal 2 and selects at random a sequence of least significant digits that are to be changed. Means 3 generates a pseudo-random sequence of binary digits and unit 4 injects these into the recorded material in place of the randomly selected least significant digits.

The output 5 from the encoder is the original digitally recorded source carrying the random identification sequence at the randomly selected locations.

Figure 4 shows a "decoding" apparatus in which a recording suspected of being a copy of the encoded recording is fed into a selector unit 11, which examines sequences of digits, the digits of which are separated by the known random time intervals. The so selected sequences are compared in unit 10 with the random or pseudo-random identifying sequence held in store 12. Copying of the source material is signified by the detection of a pre-selected high incidence of identical occurrences between the two.

When applied to delta modulated sources, in which all digits are equally significant, the method of the invention requires no significant modification: the digits replaced would still be selected on a random or pseudo-random time interval basis and the injected digit still selected from a random or pseudo-random sequence of identification digits.

In the more complex, and therefore inherently more secure, embodiments of the invention in which combinations of digits of lower significance may be replaced, the decoder would have to be able to detect combinations of the encoded digits. However, this is a matter simply of complexity rather than of real practical difficulty in realisation.

In general terms the format of the digital source is of little significance in this invention. It is simply required that the decoder be capable of detecting the locations where identifying digits would be expected to occur and comparing the digits found at these locations with a stored copy of the identifying sequence which was used in the encoding process. A high degree of coincidence between the detected sequence and the stored sequence signifies copying of the source material.

CLAIMS

1. A method of inserting an identification code in digitally recorded material, comprising;

selecting binary word locations in the digitally recorded source material and replacing at least one insignificant digit of each selected digital word with a respective replacement digit taken from an independently generated sequence.

2. A method according to claim 1 in which the binary word locations are selected at equal time intervals, or in accordance with a predetermined repeating sequence of time intervals.

3. A method according to claim 1 in which the binary word locations are selected in accordance with a predetermined random or pseudo-random sequence of time intervals.

4. A method according to any preceding claim in which the independently generated sequence comprises a series of replacement digits which all have the same value or form a regularly repeated pattern.

5. A method according to any of claims 1 to 3 in which the independently generated sequence is a random or pseudo-random sequence.

6. A method according to claim 4 or claim 5 in which original digits of corresponding significance are replaced in each word.

7. A method according to claim 2 in which the said original digits are the least significant digits.

8. A method according to claim 4 or claim 5 in which the selection of the original insignificant digit or digits to be replaced in each word, is determined by a further random or pseudo-random sequence.

9. A method of inserting an identification code in digitally recorded material, comprising the further steps of repeating the selection and replacement process of claim 1; and replacing insignificant digits of the selected words using the method of any one of claims 2 to 8.

10. A method of inserting an identification code in digitally recorded material consisting of a series of bits of equal but low significance, the method comprising selecting bits in accordance with a first predetermined random or pseudo-random sequence and replacing the selected digits with digits obtained from a second random or pseudo-random sequence.

11. Apparatus for encoding digitally recorded material for identification purposes, said apparatus comprising:

means for selecting at least one set of binary word locations in the source material and means for replacing at least one insignificant digit of each selected digital word, with a respective predetermined replacement digit.

12. Apparatus according to claim 11 further comprising: means for generating further random or pseudo-random sequences, for generating the said replacement digits and/or for determining the selection of digits to be replaced in each word.

13. Apparatus for decoding digital recordings which have been encoded using the apparatus of claim 11 or claim

12; the decoding apparatus comprising means for detecting those insignificant digits which have been replaced in the encoding process, means for holding a copy of the sequence of replacement digits used in the encoding, means for comparing the located insignificant digits with the held copy of the identifying sequence, and means for detecting a pre-selected level of agreement therebetween.

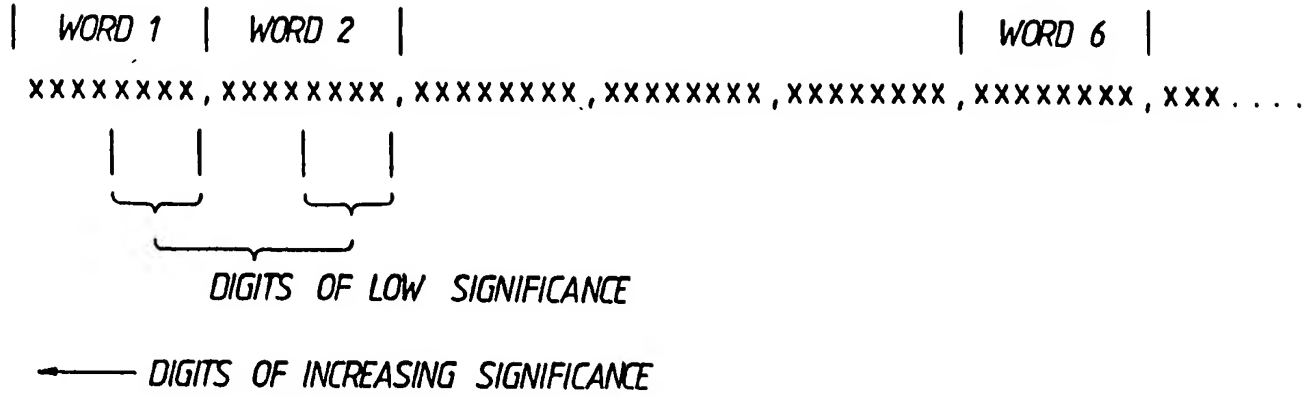


Fig.1.

CHANGED DIGITS : 5, 7, 8, 15, 16, 48

Fig.2.

PCT/GB89/00293

2/2

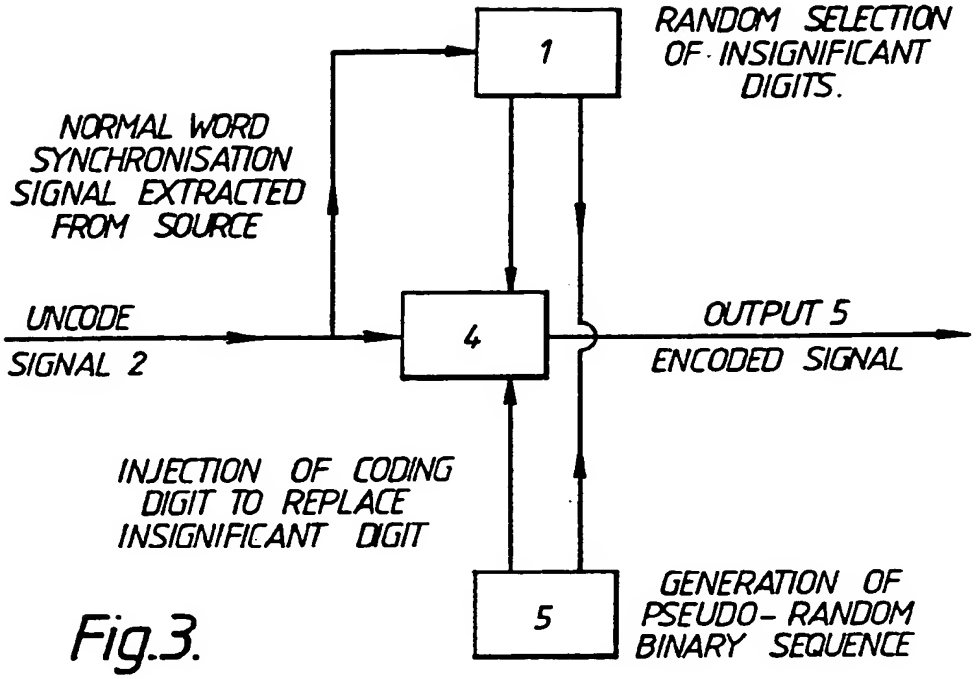

1
RANDOM SELECTION OF INSIGNIFICANT DIGITS.
NORMAL WORD SYNCHRONISATION SIGNAL EXTRACTED FROM SOURCE
UNCODE SIGNAL 2
4
OUTPUT 5 ENCODED SIGNAL
INJECTION OF CODING DIGIT TO REPLACE INSIGNIFICANT DIGIT
5
GENERATION OF PSEUDO-RANDOM BINARY SEQUENCE

Fig.3.

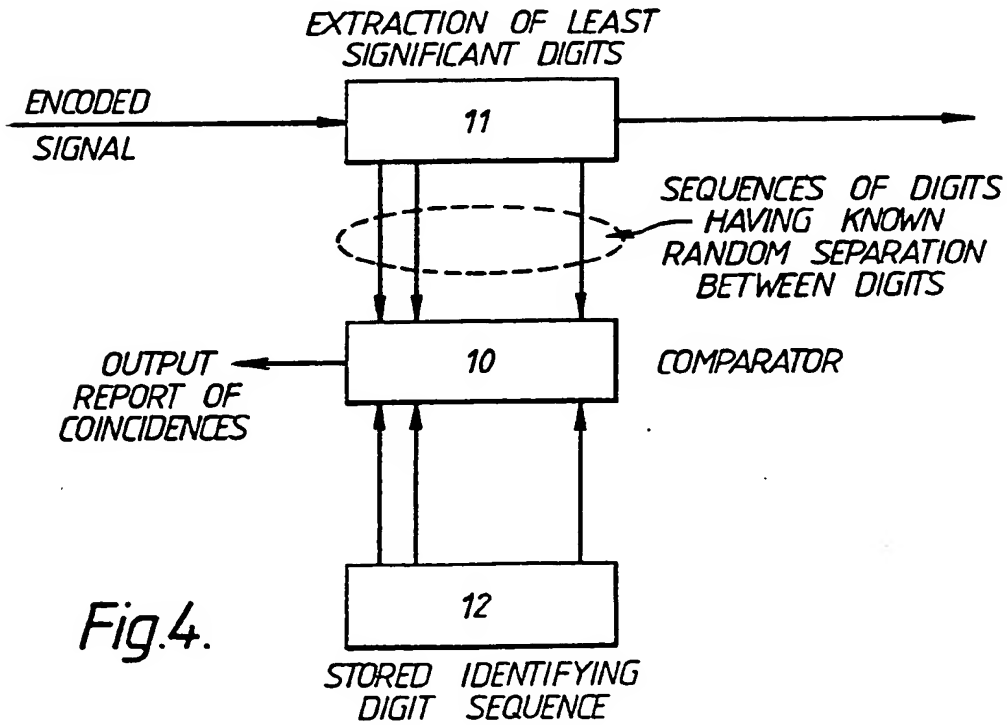

EXTRACTION OF LEAST SIGNIFICANT DIGITS
ENCODED SIGNAL
11
SEQUENCES OF DIGITS HAVING KNOWN RANDOM SEPARATION BETWEEN DIGITS
OUTPUT REPORT OF COINCIDENCES
10
COMPARATOR
12
STORED IDENTIFYING DIGIT SEQUENCE

Fig.4.

INTERNATIONAL SEARCH REPORT

293

International Application No PCT/GB 89/00239

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC4: G 11 B 20/10

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC4	G 11 B

Documentation Searched other than Minimum Documentation to the Extent that such Documents are included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
X	EP, A1, 205200 (POLYGRAM GMBH) 17 December 1986, see page 11, line 1 - page 13, line 22; figures 1,2 --	1,2,7, 11
A	EP, A2, 224929 (SONY CORPORATION) 10 June 1987, see column 5, line 5 - line 15; column 10, line 1 - line 12 --	1,2,4,6, 7,11, 13
A	EP, A1, 58482 (BRITISH TELECOMMUNICATIONS) 25 August 1982, see page 7, line 16 - page 8, line 25 --	1,2,4,6, 7,11, 13
A	EP, A1, 79669 (TOKYO SHIBAURA DENKI KABUSHIKI KAISHA) 25 May 1983, see page 4, line 26 - page 5, line 14 --	1-13

---

* Special categories of cited documents: [14]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
27th June 1989	25. 07. 89
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	P.C.G. VAN DER PUTTEN

ANNEX TO THE INTERNATIONAL SEARCH REPORT
ON INTERNATIONAL PATENT APPLICATION NO. PCT/GB 89/00293

SA 27848

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report.
The members are as contained in the European Patent Office EDP file on 03/03/89
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A1- 205200	17/12/86	DE-A-	3523809	27/11/86
		JP-A-	62026672	04/02/87
		US-A-	4750173	07/06/88
EP-A2- 224929	10/06/87	JP-A-	62132233	15/06/87
		US-A-	4775901	04/10/88
EP-A1- 58482	25/08/82	NONE		
EP-A1- 79669	25/05/83	JP-A-	58085938	23/05/83
		US-A-	4512006	16/04/85

EPO FORM P0479

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82